

AMENDMENTS TO THE CLAIMS

M. 1. (Amended) A backup/recovery system for protecting a computer system, said backup/recovery system being is installed in said computer system, said computer system including an application layer, said application layer being coupled to an interface and operating predetermined application programs, said backup/recovery system BEING CHARACTERIZED BY

- a detecting module, located within said computer system, for monitoring a predetermined messagedata;

Wherein wherein said detecting module retrieves said predetermined datamessage, in order to determine whether there is a predetermined harmful data contained therein for judging said backup/recovery system to backup data in said computer system or not, said interface implements a predetermined procedure thereafter and said application layer involves reading accessing said predetermined datamessage.

2. (Amended) The system of claim 1 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communications communication link.

3. (Original) The system of claim 2 wherein said network device is coupled to a server device.

N.E.
4. (Amended) The system of claim 3 wherein said server device is capable of controlling said client device's backup/recovery ~~conduct operation remotely and~~ immediately.

5. (Original) The system of claim 2 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

6. (Original) The system of claim 2 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

7. (Amended) The system of claim 1 wherein said predetermined harmful data comprises a file which is of a type that can contain viruses, such as in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP extension fileform.

8. (Amended) A method for protecting a computer system, said method comprising:

- Retrieving a predetermined data message to be downloaded to said computer system;

- Determining whether there being a predetermined harmful data contained in said predetermined datamessage; and;
- Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined datamessage.

9. (Amended) The method of claim 8 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communications communication link.

10. (Original) The method of claim 9 wherein said network device is coupled to a server device.

11. (Amended) The method of claim 10 wherein said server device is capable of controlling said client device's backup/recovery ~~conduct~~operation remotely and immediately.

12. (Original) The method of claim 9 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

13. (Original) The method of claim 9 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

14. (Amended) The method of claim 8 wherein said predetermined harmful data comprises a file which is of a type that can contain viruses, such as in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP extension fileform.

15. (Amended) A method for protecting a computer system with a backup/recovery system, said computer system including an application layer, said application layer coupled to an interface and operating predetermined application programs, said method comprising:

- Installing said backup/recovery system in said computer system, said backup/recovery system having a detecting module for monitoring a predetermined data message arrived to located within said computer system;
- Retrieving said predetermined datamessage to be downloaded to said computer system;
- Determining whether there being a predetermined harmful data contained in said predetermined datamessage;
- Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined datamessage;
- Implementing a predetermined procedure by said interface; and

- Indicating said application layer read-access said predetermined message.

16. (Amended) The method of claim 15 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communication communications link.

17. (Original) The method of claim 16 wherein said network device is coupled to a server device.

18. (Amended) The method of claim 17 wherein said server device is capable of controlling said client device's backup/recovery conduct operation remotely and immediately.

19. (Original) The method of claim 16 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

20. (Original) The method of claim 16 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.